Codes with locality from cyclic extensions of Deligne-Lusztig curves

Gretchen L. Matthews[1][0000−0002−8977−8171]
and Fernando Piñero[2][0000−0002−9714−7249]

Department of Mathematics, Virginia Tech, Blacksburg, VA 24061
gmatthews@vt.edu *
Department of Mathematics, University of Puerto Rico at Ponce, Ponce, PR
fernando.pinero1@upr.edu

Abstract. Recently, Skabelund defined new maximal curves which are cyclic extensions of the Suzuki and Ree curves. Previously, the now well-known GK curves were found as cyclic extensions of the Hermitian curve. In this paper, we consider locally recoverable codes constructed from these new curves, complementing that done for the GK curve. Locally recoverable codes allow for the recovery of a single symbol by accessing only a few others which form what is known as a recovery set. If every symbol has at least two disjoint recovery sets, the code is said to have availability. Three constructions are described, as each best fits a particular situation. The first employs the original construction of locally recoverable codes from curves by Tamo and Barg. The second yields codes with availability by appealing to the use of fiber products as described by Haymaker, Malmskog, and Matthews, while the third accomplishes availability by taking products of codes themselves. We see that cyclic extensions of the Deligne-Lusztig curves provide codes with smaller locality than those typically found in the literature.

1 Introduction

Maximal curves have played a role in a number of applications in coding theory. For instance, they allow for the construction of long algebraic geometry codes and yield explicit families of codes with parameters exceeding the Gilbert-Varshamov bound [23]. The Deligne-Lusztig curves, which include the Hermitian, Suzuki, and Ree curves, have proven particularly useful. In particular, Hermitian codes are perhaps the best understood algebraic geometry codes other than Reed-Solomon codes. The Suzuki and Ree curves share several important properties with the Hermitian family in that they are optimal with respect to the Hasse-Weil bound and have known automorphism groups; thus, codes from these curves have interesting properties as well.

More recently, maximal curves have been employed in the construction of codes with locality. In some applications, it is desirable to recover a single (or

---

small number of) codeword symbol(s) by accessing only a few, say r, particular symbols of the received word. This leads to the notion of locally recoverable codes, or LRCs. Tamo and Barg [21] introduced a construction for codes with locality that is similar to that of algebraic geometry codes. This motivated much work on locally recoverable codes, including [1], [2], [7], [11], [13]. In [9], we employ maximal curves to construct LRCs with availability $t \geq 2$, meaning each coordinate j has t disjoint recovery sets. Codes with availability make information more available to more users, since recovery of an erasure is not entirely dependent on a single set of coordinates (which may itself contain erasures).

In this paper, we define codes with locality from new maximal curves constructed by Skabelund [18] using cyclic covers of the Suzuki and Ree curves. The Suzuki curve S_q over $\mathbb{F}_q$ gets its name from its automorphism group which is the Suzuki group $Sz(q)$ of order $q^2(q^2 + 1)(q - 1)$. In [8], Hansen and Stichtenoth considered this curve and applications to algebraic geometry codes leading to other works such as [12], [15]. Recently, Eid, Hammond, Ksir, and Peachey [4] constructed an algebraic geometry (AG) code over $\mathbb{F}_{q^4}$ whose automorphism group is $Sz(q)$. Skabelund considers a cyclic extension of S_q and proves it is maximal over $\mathbb{F}_q$ and $\mathbb{F}_{q^4}$. Similarly, the Ree curve R_q over $\mathbb{F}_q$ has a Ree group as its automorphism group. Both curve constructions are similar to that of the Giulietti-Korchmáros, or GK, curve, which has already proven useful in constructing codes with locality. These cyclic extensions of the Suzuki and Ree curves have also been utilized for AG codes and for quantum codes from them [16] and their automorphism groups have been determined by Giulietti, Montanucci, Quoos, and Zini [6].

This paper is organized as follows. In Section 2, we obtain codes with locality from the cyclic extension $\tilde{S}_q$ of the Suzuki curve S_q and the cyclic extension $\tilde{R}_q$ of the Ree curve R_q. The locality is much smaller relative to the alphabet size and code length than comparable constructions. In Section 3, we construct codes with availability from $\tilde{S}_q$ and $\tilde{R}_q$. Our constructions build on tools found in [21] and [9], and some useful background may be found there. Because explicit code descriptions remain out of reach for these standard constructions when employing R_q or $\tilde{R}_q$ (as they depend on explicit bases for Riemann-Roch spaces which remain elusive), we provide an alternate construction for such settings. We also consider constructions from products of codes. In Section 4, we consider examples of the above constructions and make some comparisons between them.

2   Locally recoverable codes

Locally recoverable codes, or LRCs for short, can recover a single (or small number of) codeword symbol(s) by accessing a small number, say r, of particular symbols of the received word. In principle, the locality r should be small so as to limit network traffic though this can adversely impact other code parameters. While an $[n, k, d]$ code C, meaning a code of length n, dimension k, and minimum distance d, can recover any $d-1$ erasures or correct any $\left\lfloor \frac{d-1}{2} \right\rfloor$ errors, this assumes access to all other symbols of the entire received word. More precisely, the code

C of length n over the alphabet $\mathbb{F}$ (typically taken to be a finite field) is locally recoverable with locality r if and only if for all $j \in [n] := \{1, \ldots, n\}$ there exists

$$A_j \subseteq [n] \setminus \{j\} \text{ with } |A_j| = r$$

and

$$c_j = \phi_j(c|_{A_j})$$

for some function

$$\phi_j : A_j \to \mathbb{F}$$

for all $c \in C$. The set A_j is called a recovery set for the j-th coordinate. In this section, we see how cyclic extensions naturally lead to LRCs.

2.1   LRCs from cyclic extensions of Suzuki curves

The Suzuki curve S_q may be described by the equation

$$S_q : y^q + y = x^{q_0} (x^q + x)$$

where $q_0 = 2^s$, $q = 2q_0^2$, and $s \in \mathbb{N}$. It is an optimal curve over $\mathbb{F}_q$, having $q^2 + 1$ $\mathbb{F}_q$-rational points. Indeed, if $a, b \in \mathbb{F}_q$, $a^q = a$ and $b^q = b$; since char $\mathbb{F}_q = 2$, $b^q + b = 0 = a^{q_0}(a^q + a)$. In addition, there is a unique point at infinity P_∞ corresponding to $x = z = 0$ and $y = 1$. The genus of S_q is $q_0(q - 1)$ [8, Lemma 1.9]. It is maximal over $\mathbb{F}_{q^4}$, having $q^4 + 1 + 2q_0 q^2(q - 1)$ $\mathbb{F}_{q^4}$-rational points [4, Equation (7)]. Define

$$\tilde{S}_q : \begin{cases} y^q + y = x^{q_0} (x^q + x) \\ t^m = x^q + x. \end{cases}$$

where $m = q - 2q_0 + 1$. The curve $\tilde{S}_q$ has a unique point at infinity, and affine points will be denoted $P_{abc} := (a : b : c : 1)$ to mean the unique zero of $x - a$, $y - b$, and $t - c$, just as those of S_q will be denoted by P_{ab}. The genus of $\tilde{S}_q$ is $\frac{q^3 - 2q^2 + q}{2}$ [18]. According to [18], the number of $\mathbb{F}_{q^4}$-rational points on $\tilde{S}_q$ that are not $\mathbb{F}_q$-rational is

$$q^5 - q^4 + q^3 - q^2;$$

see also [18, Section 3] for a discussion of the points on this curve. Define

$$\begin{aligned} g : \tilde{S}_q &\to S_q \\ P_{abc} &\mapsto P_{ab} \end{aligned}$$

Let

$$S := S_q\left(\mathbb{F}_{q^4}\right) \setminus S_q\left(\mathbb{F}_q\right). \tag{1}$$

Then $|S| = q^4 + 2q_0 q^2(q-1) - q^2$ [4, Equations (4)-(7)]. Set $D := \sum_{P \in \mathcal{D}} P$ where

$$\mathcal{D} := g^{-1}(S) = \left\{ P_{abc} \in \tilde{S}_q\left(\mathbb{F}_{q^4}\right) : c \neq 0 \right\}. \tag{2}$$

For each $P_{ab} \in S$, $g^{-1}(P_{ab}) = \{P_{abc} : c^m = a^q + a\}$, so

$$|g^{-1}(P_{ab})| = q - 2q_0 + 1. \tag{3}$$

Recall that given a divisor G on a curve X over a field $\mathbb{F}$, the space of functions determined by G, sometimes called the Riemann-Roch space of G, is

$$\mathcal{L}(G) := \{f \in \mathbb{F}(X) : (f) \geq -G\} \cup \{0\},$$

where $\mathbb{F}(X)$ denotes the set of rational functions on X, and (f) denotes the divisor of the function f; to say that $(f) = \sum_{Q \in \mathcal{Z}} a_Q Q - \sum_{P \in \mathcal{P}} b_P P$ with $a_Q, b_P \in \mathbb{Z}^+$ means f has a zero of order a_Q at Q and a pole of order b_P at P. We use the standard notation $(f)_0 := \sum_{Q \in \mathcal{Z}} a_Q Q$ to denote the zero divisor of f and $(f)_\infty := \sum_{P \in \mathcal{P}} b_P P$ to denote the pole divisor of f. Let $\alpha \in \mathbb{Z}^+$, and consider the divisor

$$G := \alpha \left(P_\infty + \sum_{a,b \in \mathbb{F}_q} P_{ab} \right)$$

on S_q. It is worth noting that $\mathcal{L}\left(\alpha \left(P_\infty + \sum_{a,b \in \mathbb{F}_q} P_{ab} \right) \right) \cong \mathcal{L}\left(\alpha \left(q^2 + 1 \right) P_\infty \right)$ [4]. According to [4, Theorem 1], a basis for $\mathcal{L}(G)$ is given by

$$\mathcal{B} := \left\{ \frac{x^a y^b u^c v^d}{(x^q + x)^e} : \begin{array}{l} aq + b(q + q_0) + c(q + 2q_0) \\ \quad + d(q + 2q_0 + 1) \leq \alpha + eq^2 \\ a \in \{0, \ldots, q-1\}, b \in \{0, 1\}, \\ c, d \in \{0, \ldots, q_0 - 1\}, e \in \{0, \ldots, \alpha\} \end{array} \right\} \subseteq \mathbb{F}_{q^4}(S_q)$$

where

$$u = x^{2q_0 + 1} - y^{2q_0}$$

and

$$v = xy^{2q_0} - u^{2q_0}.$$

Set

$$V := \left\langle ft^i : i = 0, \ldots, m - 2; f \in \mathcal{B} \right\rangle_{\mathbb{F}_{q^4}}.$$

Now define

$$ev : V \to \mathbb{F}_{q^4}^{(q - 2q_0 + 1)\left(q^4 + 2q_0 q^2 (q-1) - q^2\right)}$$
$$f \mapsto \left(f(P_{abc}) \right)_{P_{abc} \in \tilde{S}_q(\mathbb{F}_{q^4}) \setminus \tilde{S}_q(\mathbb{F}_q)},$$

and set $C(D, G, g) := ev(V)$. Note that the evaluation map ev is well-defined, as $|\mathcal{D}| = (q - 2q_0 + 1)(q^4 + 2q_0 q^2(q-1) - q^2)$ and $f \in V$ has no poles at points in $\mathcal{D}$. One may notice that

$$V \subseteq \mathcal{L}\left(\left(m\alpha + (m-2)q^2 \right) \tilde{P}_\infty + m\alpha \sum_{a,b \in \mathbb{F}_q} P_{a,b,0} \right) \tag{4}$$

where $\tilde{P}_\infty$ denotes the unique point of $\tilde{S}_q$ lying above P_∞. Let

$$G' := \left(m\alpha + (m-2)q^2\right)\tilde{P}_\infty + m\alpha \sum_{a,b \in \mathbb{F}_q} P_{a,b,0}.$$

We are now ready to state the result.

Theorem 1. *Suppose $C(D,G,g)$ is constructed as above where $\deg G' < |S|$. Then $C(D,G,g)$ is an $[n,k,d]$ code over $\mathbb{F}_{q^4}$ with locality $q - 2q_0$,*

$$n = (q - 2q_0 + 1)\left(q^4 + 2q_0q^2(q-1) - q^2\right),$$

$$k = (q - 2q_0)\left(\alpha\left(q^2 + 1\right) - q_0(q-1) + 1\right),$$

and

$$d \geq n - \left(m\alpha q^2 + m\alpha + (m-2)q^2\right).$$

Proof. The map ev is injective, since $\deg G' < |S|$ guarantees the kernel of the evaluation map is $\{0\}$; this may be observed by noting that if $f \in \ker ev \setminus \{0\}$ then f would have more zeros than poles. Hence, the dimension is given by $\dim_{\mathbb{F}_{q^4}} V$ which follows from the facts that $\{t^i : i = 0, 1, \ldots, m-1\}$ is a basis of $\mathbb{F}_{q^4}(\tilde{S}_q)/\mathbb{F}_{q^4}(S_q)$; $\mathcal{B}$ is a basis for $\mathbb{F}_{q^4}(S_q)/\mathbb{F}_{q^4}$; and

$$|\mathcal{B}| = \left(\alpha\left(q^2 + 1\right) - q_0(q-1) + 1\right)$$

according to [4, Remark 1]. We claim that $R := g^{-1}(P_{ab}) \setminus \{P_{abc}\}$ is a recovery set for the position corresponding to P_{abc}. Suppose $f \in V$. Then

$$f(x,y,t) = \sum_{i=0}^{m-2} \sum_{j=1}^{M} a_{ij} f_j^* t^i$$

for some $a_{ij} \in \mathbb{F}_{q^4}$ and $f_j^* \in \mathcal{B}$, where $M := |\mathcal{B}|$. Notice that $f(a,b,T) \in \mathbb{F}_q[T]$ and $\deg_T f(a,b,T) \leq m - 2$. Hence, $f(a,b,c)$ can be recovered using the $m - 1$ interpolation points: $P_{abc'} \in R$. As a result, $f(P_{abc})$ may be recovered using only elements of R.

To determine a bound on the minimum distance d, we use that

$$d \geq wt(ev(h)) \geq n - \deg(h)_0$$

where $h = ft^{m-2}$ and $f \in \mathcal{B} \subseteq \mathcal{L}(G)$. Then $\deg(h)_0 \geq m\deg(G) + (m-2)q^2 \geq m\alpha(q^2+1) + (m-2)q^2$ as G is a divisor of degree $\alpha(q^2+1)$ on S_q, $[\tilde{S}_q : S_q] = m$, and (t) is a divisor on $\tilde{S}_q$ with zero divisor of degree q^2. As a result

$$d \geq n - \left(m\alpha(q^2 + 1) + (m-2)q^2\right).$$

Alternatively, the bound on the minimum distance may be seen as a consequence of $d \geq n - \deg G'$ using (4).

Example 1. Let $q = 8$ and $q_0 = 2$, so $q^4 = 4096$. Notice that the Suzuki curve

$$S_8 : y^8 + y = x^2 \left(x^8 + x \right)$$

has 64 $\mathbb{F}_8$-rational points and 5888 $\mathbb{F}_{4096}$-rational points. Here, $|S| = 5824$ and $n = 29120$. Then $C(D, G, g)$ has locality 4. We can compare this with an LRC C' from the Hermitian curve $y^{64} + y = x^{65}$ over the same field, $\mathbb{F}_{4096}$. Using a projection onto the x-coordinate gives a code of length 262144 with locality 63 whereas projection onto the y-coordinate yields locality 64. Hence, the construction using $\tilde{S}_8$ has a smaller ratios of locality to code length and to alphabet size.

Remark 1.   1. Other bounds on the minimum distance of the codes in Theorem 1 may be given; see [22] for instance.
  2. Alternatively, an LRC may be constructed using the projection

$$g : \begin{array}{l} \tilde{S}_q \to C_m \\ P_{abc} \mapsto Q_{ac} \end{array}$$

where C_m denotes the curve given by $t^m = x^q + x$ and Q_{ac} denotes the common zero of $x - a$ and $t - c$. Let S be as in (1), D as in (2), and $G' := \alpha Q_\infty$ where Q_∞ is the point at infinity on C_m. Then a basis for $\mathcal{L}\left(\alpha Q_\infty \right)$ is given by

$$\mathcal{B}' := \left\{ t^i x^j : i \geq 0, j \in \{0, \ldots, q - 1\}, qi + mj \leq \alpha \right\};$$

see, for instance, [10, Lemma 12.2(i)]. Use this to define

$$V = \left\langle f y^i : i \in \{0, \ldots, q - 2\}, f \in \mathcal{B}' \right\rangle.$$

The code $C(D, G', g)$ has locality $q - 1$ and dimension $(q - 1) |\mathcal{B}|$.

In Section 3, we will see how these two approaches can be combined to give LRCs with availability. Before doing so, we turn our attention to cyclic extensions of Ree curves.

2.2   LRCs from cyclic extensions of Ree curves

The Ree curve R_q may be described by the equation

$$R_q : \begin{cases} y^q - y = x^{q_0} \left(x^q - x \right) \\ z^q - z = x^{2q_0} \left(x^q - x \right) \end{cases}$$

where $q_0 = 3^s$, $q = 3q_0^2$, and $s \in \mathbb{N}$. It is optimal over $\mathbb{F}_{q^6}$. In addition, there is a unique point at infinity. The genus of R_q is $\frac{3}{2} q_0 (q - 1)(q + q_0 + 1)$ [8]. Define

$$\tilde{R}_q : \begin{cases} y^q - y = x^{q_0} \left(x^q - x \right) \\ z^q - z = x^{2q_0} \left(x^q - x \right) \\ t^m = x^q - x \end{cases}$$

where $m = q - 3q_0 + 1$. The curve $\tilde{R}_q$ has a unique point at infinity, and affine points will be denoted $P_{abcd} := (a : b : c : d : 1)$ to mean the unique zero of $x - a$, $y - b$, $z - c$ and $t - d$, just as those of R_q will be denoted by P_{abc}. The genus of $\tilde{R}_q$ is $\frac{q^4 - 2q^3 + q}{2}$. According to [16], the number of $\mathbb{F}_{q^6}$-rational points on $\tilde{R}_q$ that are not $\mathbb{F}_q$-rational is

$$q^7 - q^6 + q^4 - q^3;$$

see also [18]. Define

$$g : \begin{array}{ccc} \tilde{R}_q & \to & R_q \\ P_{abcd} & \mapsto & P_{abc} \end{array}$$

and let

$$S := R_q\left(\mathbb{F}_{q^6}\right) \setminus R_q\left(\mathbb{F}_q\right). \tag{5}$$

Set $D := \sum_{P \in \mathcal{D}} P$ where

$$\mathcal{D} := g^{-1}(S) = \left\{ P_{abcd} \in \tilde{R}_q\left(\mathbb{F}_{q^6}\right) : d \neq 0 \right\}. \tag{6}$$

For each $P_{abc} \in S$, $g^{-1}(P_{abc}) = \{P_{abcd} : d^m = a^q - a\}$, so

$$|g^{-1}(P_{abc})| = q - 3q_0 + 1. \tag{7}$$

Consider the divisor $G = \alpha P_\infty$ on R_q with $m \deg G + (m-2) \deg(t)_\infty < |S|$. Set

$$V := \left\langle ft^i : i = 0, \ldots, m-2; f \in \mathcal{L}(G) \right\rangle_{\mathbb{F}_{q^6}}.$$

Now define

$$\begin{array}{l} ev : V \to \mathbb{F}_{q^6}^{|\mathcal{D}|} \\ f \mapsto (\tilde{f}(P_{abcd}))_{P_{abcd} \in \tilde{R}_q\left(\mathbb{F}_{q^6}\right) \setminus \tilde{R}_q(\mathbb{F}_q)}, \end{array}$$

and set $C(D, G, g) := ev(V)$.

Proposition 1. *Suppose $C(D, G, g)$ is constructed as above. Then $C(D, G, g)$ is an $[q^7 - q^6 + q^4 - q^3, (m-1)\ell(G)]$ code over $\mathbb{F}_{q^6}$ with locality $q - 3q_0$.*

Proof. This follows similarly to that of Theorem 1.

Remark 2. 1. Explicit bases for $\mathcal{L}(G)$ where G is a divisor on the Ree curve is a topic of current research for arbitrary q, even for the case where G is a multiple of the point at infinity. See [19] for recent work on related topics. The work [3] also highlights the challenges of this problem, which was originally stated in [17]; indeed, when $s = 1$ (so $q = 27$), the associated Weierstrass semigroup has more than 100 generators, compared with 2 in the Hermitian case and 4 for Suzuki. Hence, the dimension of the codes described in Proposition 1 cannot be specified more precisely the expression given above for arbitrary q. However, for specific small values of q, a set of functions which generate $\mathcal{L}(G)$ may be found computationally. We include this result so that if the theory progresses and sheds more light on this value, LRCs are an immediate consequence. We also note that our interest in the Ree

curve is partially motivated by the fact that it allows for results over fields of odd characteristic whose cardinalities are odd powers of primes (unlike the Suzuki curve, which is considered over a field of even characteristic, and the Hermitian curve which is considered over a field with square cardinality).

2. Also, as in Remark 1, the projection

$$g: \quad \tilde{R}_q \quad \to C_m$$
$$P_{abcd} \mapsto Q_{ad},$$

where $C_m : t^m = x^q - x$ and Q_{ad} denotes the common zero of $x - a$ and $t - c$, may be used to define a code with different recovery sets than those considered above.

3. A bound on the minimum distance is given in [9, Theorem 3.1]

3   Locally recoverable codes with availability from products

3.1   Availability from cyclic extensions viewed as fiber products of curves

If every coordinate j has t disjoint recovery sets, then C is said to have availability t to reflect that information is more available to users in the presence of erasure. In [9], fiber products of curves are used to construct locally recoverable codes with availability. We review the construction in the case $t = 2$ below.

Suppose $X = Y_1 \times_Y Y_2$ where Y_1, Y_2, and Y are curves over a finite field $\mathbb{F}$ with rational, separable maps $h_i : Y_i \to Y$. The $\mathbb{F}_q$-rational points of X are $\{(P_1, P_2) : P_i$ is an $\mathbb{F}_q - $rational point on $Y_i, h_1(P_1) = h_2(P_2)\}$. Thus, there are projection maps $g_i : X \to Y_i$ defined by $g_i(P_1, P_2) = P_i$; a rational, separable map $g : X \to Y$ given by $g = h_1 \circ g_1 = h_2 \circ g_2$; maps of function fields $h_i^* : \mathbb{F}(Y) \to \mathbb{F}(Y_1)$ given by $h_i^*(f) := f \circ h_i$; and primitive elements x_i of the extensions $\mathbb{F}(Y_i)/h_i^*(\mathbb{F}(Y))$. Let S be a set of $\mathbb{F}$-rational points on Y, and take $D := \sum_{P \in g^{-1}(S)} P$. Choose an effective divisor G on Y of degree $\ell < |S|$, and take a basis $\{f_1, \ldots, f_t\}$ for $\mathcal{L}(G)$. Set

$$V := Span\left\{(f_i \circ g) \, x_1^{*e_1} x_2^{*e_2} : 1 \le i \le t, 0 \le e_i \le \deg h_i - 2\right\}$$

where $x_i^* = g_i^*(x_i)$ given that $g_i^* : \mathbb{F}(Y_i) \to \mathbb{F}(X)$ for $i = 1, 2$. Consider

$$ev : V \to \mathbb{F}^n$$
$$f \mapsto (f(P_i))_{P_i \in \text{supp} D}.$$

Then the code $C(D, G, g, g_1, g_2) := ev(V)$ has length $|D| = \deg g|S|$, dimension

$$t(\deg h_1 - 1)(\deg h_2 - 1),$$

and minimum distance bounded below according to [9]. For $i = 1, 2$,

$$g_i^{-1}(g_i(Q)) \setminus \{Q\}$$

serves as a recovery set for $Q \in S$. Hence, $C(D, G, g, g_1, g_2)$ has locality 2. Next we apply this construction to $\tilde{S}_q$ and $\tilde{R}_q$.

Cyclic extensions of Suzuki curves as fiber products. Because $\tilde{S}_q$ is the fiber product of covers $S_q \to \mathbb{P}_x^1$ and $C_m \to \mathbb{P}_x^1$, we may apply the construction to obtain a code with availability 2 and localities $m - 1$ and $q - 1$; that is, every coordinate has 2 disjoint recovery sets, one of cardinality $q - 2q_0$ and one of cardinality $q - 1$. To do this, consider the projection maps $g_1 : \tilde{S}_q \to C_m$, $g_2 : \tilde{S}_q \to S_q$, and $g : \tilde{S}_q \to \mathbb{P}_x^1$. We take S as in (1), D as in (2), and $G := \alpha P_\infty$ where P_∞ is the unique point at infinity on $\mathbb{P}_x^1$. Fix a basis $\mathcal{B}$ of $\mathcal{L}(G)$, and

$$V := \left\langle f y^i t^j : 0 \leq i \leq q - 2, 0 \leq j \leq m - 2, f \in \mathcal{B} \right\rangle_{\mathbb{F}_{q^4}}.$$
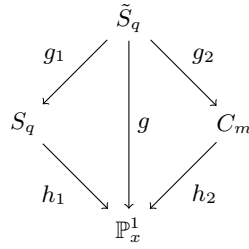
Fig. 1. Cyclic extension of Suzuki curve viewed as a fiber product

Theorem 2. *Suppose $C(D, G, g, g_1, g_2)$ is constructed as above. Then the code $C(D, G, g, g_1, g_2)$ is an $[n, k, d]$ code over $\mathbb{F}_{q^4}$ with availability 2 and recovery sets for each coordinate of sizes $q - 2q_0$ and $q - 1$, where*

$$n = (q - 2q_0 + 1) \left(q^4 + 2q_0 q^2 (q - 1) - q^2 \right),$$

$$k = (q - 2q_0) (\alpha + 1) (q - 1),$$

and

$$d \geq n - \left(\alpha m q + (q - 2) m (q + q_0) + (m - 2) q^2 \right).$$

Proof. The length and dimension can be verified directly by applying [9, Theorem 3.1]. To determine the minimum distance d, we use the fact that $d \geq n - wt(ev(h)) \geq n - \deg(h)_0$ where $h = f y^{q-2} t^{m-2}$ and $f \in \mathcal{L}(\alpha P_\infty)$. Then $(h) = (f) + (q - 2)(y) + (m - 2)(t)$. Note that when considered as a functions on $\tilde{S}_q$, $\deg(f)_0 \leq \alpha m q$, $\deg(y)_0 \leq m(q + q_0)$, and $\deg(t)_0 \leq q^2$. Putting this together, we conclude that $d \geq n - \left(\alpha m q + (q - 2) m (q + q_0) + (m - 2) q^2 \right)$, which coincides with that given in [9, Theorem 3.1].

We claim that

$$R^{(1)} := g_2^{-1} \left(g_2 \left(P_{abc} \right) \right) \setminus \{ P_{abc} \} = \left\{ P_{ab'c} : b' \in \mathbb{F}_{q^4} \setminus \{ b \} \right\}$$

and

$$R^{(2)} := g_1^{-1} \left(g_1 \left(P_{abc} \right) \right) \setminus \{ P_{abc} \} = \left\{ P_{abc'} : c' \in \mathbb{F}_{q^4} \setminus \{ c \} \right\}$$

are recovery sets for the position corresponding to P_{abc}. Suppose $f \in V$. Then $f(x,y,t) = \sum_{i=0}^{m-2} \sum_{j=1}^{M} a_{ij} f_j^* t^i$. Notice that $f(a,b,T) \in \mathbb{F}_q[T]$ and the degree is bounded by $\deg_T f(a,b,T) \le m - 2$. Hence, $f(a,b,c)$ can be recovered using the $m-1$ interpolation points: $P_{abc'} \in R$. As a result, $f(P_{abc})$ may be recovered using only elements of R.

Observe that the functions in the set V are modified from the construction in Section 2 in order to obtain multiple recovery sets for each position, thus impacting the dimension of the code.

One might compare this with the code found in [9, Theorem 6.1], which has availability 2 with recovery sets of size $q-1$, length $n = q(q-1)(q^2 + 2qq_0 + q + 1)$ and dimension $k = (q-1)(q-2)(q^2 + 2qq_0 + q + 1)$. Notice that the new codes defined using $\tilde{S}_q$ give the option of using a smaller recovery set (cardinality $q - 2q_0$ compared with $q - 1$).

Cyclic extensions of Ree curves as fiber products. Because $\tilde{R}_q$ is the fiber product of $R_q \to \mathbb{P}_x^1$ and $C_m \to \mathbb{P}_x^1$, we may apply this construction to obtain a code with availability 2 and localities $m-1$ and $q-1$; that is, every coordinate has 2 disjoint recovery sets, one of cardinality $q - 3q_0$ and one of cardinality $q - 1$. To do this, consider the projection maps $g_1 : \tilde{R}_q \to C_m$, $g_2 : \tilde{R}_q \to R_q$, and $g : \tilde{R}_q \to \mathbb{P}_x^1$. We take S as in (5), D as in (6), and G is a divisor on $\mathbb{P}_x^1$. Fix a basis $\mathcal{B}$ of $\mathcal{L}(G)$, and

$$V := \left\langle f y^i t^j : 0 \le i \le q - 2, 0 \le j \le q - 3q_0 - 1, f \in \mathcal{B} \right\rangle_{\mathbb{F}_{q^6}}.$$
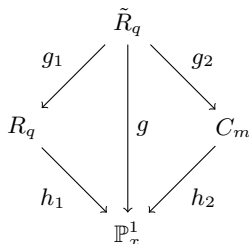
Fig. 2. Cyclic extension of Ree curve viewed as a fiber product

Proposition 2. *The code* $C(D, G, g, g_1, g_2)$ *constructed as above is a code with parameters* $[q^7 - q^6 + q^4 - q^3, \ell(G)(q-1)(q-3q_0)]$ *code over* $\mathbb{F}_{q^6}$ *with availability 2 and recovery sets for each coordinate of sizes* $q - 3q_0$ *and* $q - 1$.

Proof. The proof is similar to that of Theorem 2.

Remark 3.   1. As noted in Remark 2, the explicit construction for codes from the Ree curve depends on that of bases for certain Riemann-Roch spaces. We provide an alternate LRC with availability construction from the Ree curve in the Section 4. There, we see codes with more accessible parameters due to choosing functions to evaluate carefully, rather than beginning with an entire Riemann-Roch space which is difficult to describe.
   2. A bound on the minimum distance is given in [9, Theorem 3.1].

Observe the functions in the set V are modified from the construction in Section 2 in order to obtain multiple recovery sets for each position, thus impacting the dimension of the code.

3.2   Availability from products of codes

We may also take products of codes themselves to obtain LRCs with availability, as detailed below. We begin with the simplest definition, the product of two codes, C_1 and C_2, which may be generalized to more factors. Examples of this construction may be found in the next section.

Definition 1. *Let C_1 be an $[n_1, k_1, d_1]$ code and C_2 be an $[n_2, k_2, d_2]$ code over the same alphabet $\mathbb{F}$. The product code of C_1 and C_2 is defined by assigning symbols from $\mathbb{F}$ to the pairs $(i, j) \in [n_1] \times [n_2]$ such that the symbols assigned in $[n_1] \times \{j\}$, for $j \in [n_2]$ are a codeword in C_1 and $\{i\} \times [n_2]$ for $i \in [n_1]$ are a codeword in C_2; that is,*

$$C_1 \times C_2 := \{(a_i b_j) \in \mathbb{F}^{[n_1] \times [n_2]} \mid (a_1, a_2, \ldots, a_{n_1}) \in C_1, (b_1, b_2, \ldots, b_{n_2}) \in C_2\}$$

An alternative definition is to place symbols from $\mathbb{F}$ in an $n_1 \times n_2$ rectangular array such that each column is a codeword of C_1 and each row is a codeword of C_2. See also [14].

Theorem 3. *Let C_1 be an $[n_1, k_1, d_1]$ code and C_2 be an $[n_2, k_2, d_2]$ code. Then the code $C_1 \times C_2$ is a $[n_1 n_2, k_1 k_2, d_1 d_2]$ code with availability 2. Moreover, if C_1 has locality r_1 and availability l_1 and C_2 has locality r_2 and availability l_2, then $C_1 \times C_2$ is a code of availability $l_1 + l_2$ and locality $r_1 + r_2$.*

Proof. Let D denote the minimum distance of the code $C_1 \times C_2$. If (i, j) is a nonzero position, then there are d_1 positions in the set $[n_1] \times \{j\}$ which have a nonzero entry. Suppose those nonzero positions are $(i_1, j), (i_2, j), \ldots, (i_{d_1}, j)$. For each of those nonzero positions (i_s, j), there are d_2 nonzero positions in $\{i_s\} \times [n_2]$. Thus there are at least $d_1 d_2$ nonzero positions.

In order to prove equality, let $(a_1, a_2, \ldots, a_{n_1})$ be a codeword of weight d_1 in C_1, and $(b_1, b_2, \ldots, b_{n_2})$ be a codeword of weight d_2 in C_2. Then the codeword defined by $c_{i,j} = a_i b_j$ is the required codeword of weight $d_1 d_2$.

Let I_1 be an information set for C_1 and let I_2 be an information set of C_2. The ith coordinate of $c \in C_1$ may be written as the linear combination $\mathbf{p_i m_1}$ for a message vector $m_1 \in \mathbb{F}^{I_1}$. Likewise, the ith coordinate of $c \in C_1$ may be written

as the linear combination $\mathbf{q_j m_2}$ for a message vector $m_2 \in \mathbb{F}^{I_2}$. After placing any values in $I_1 \times I_2$, the remaining values are given by $c_{i,j} = \mathbf{p_i m_1 q_j m_2}$.

Note that position (i,j) is in the two sets $[n_1] \times \{j\}$ and $\{i\} \times [n_2]$. These two sets have only (i,j) in common. Thus, $[n_1] \times \{j\} \setminus (i,j)$ and $\{i\} \times [n_2] \setminus (i,j)$ are recovery sets for (i,j); note that they are disjoint as required for availability.

Consider $(i,j) \in [n_1] \times [n_2]$. As C_1 is a code of availability l_1 there are l_1 disjoint sets , $I_1, I,2, \ldots, I_{l_1}$ in $[n_1] \setminus \{i\}$ from which position i may be recovered. Likewise as C_2 is a code of availability l_2 there are l_2 disjoint sets , $J_1, J_2, \ldots, J_{l_2}$ in $[n_2] \setminus \{j\}$ from which position j may be recovered. The sets $I_1 \times \{j\}, I_2 \times \{j\}, \ldots,$ $I_{l_1} \times \{j\}, \{i\} \times J_1, \{i\} \times J_2, \ldots, \{i\} \times J_{l_2}$ are then $l_1 + l_2$ recovery sets which are disjoint; this gives the desired availability.

4   Examples

A number of examples of LRCs are given in this section, and some comparisons are drawn between instances of the constructions discussed in this paper as well as those appearing elsewhere in the literature. In addition, we provide LRCs on the Ree curve via a construction that allows for computable parameters despite the issues mentioned in Remarks 2 and 3.

Tamo and Barg gave a seminal construction of an optimal LRC code of locality r in [21]. The LRC construction is based on a set $L \subseteq \mathbb{F}_q$, a partition of L into disjoint subsets $A_1, A_2, \ldots, A_m$ where each set A_i has size $r+1$ and a polynomial $g(x)$ of degree $r+1$ such that g is constant on each subset A_i. Tamo and Barg construct an LRC code from a subcode of the Reed–Solomon code over L of dimension k' by evaluating the functions of the form $X^i g(X)^j$ where $0 \le i \le r, i \ne s$ for a fixed $0 \le s \le r$ and $i + (r+1)j \le k' - 1$. There are many partitions and many choices for $g(X)$. However, we shall focus on partitions given by linear subsets of $\mathbb{F}_q$ or by cosets of the multiplicative group of $\mathbb{F}_q$. We shall use evaluation codes as a generalization of Reed–Solomon codes and AG codes.

Let $A = \{\alpha_1, \alpha_2, \ldots, \alpha_n\} \subseteq \mathbb{F}_q^m$. Let $f(x_1, x_2, \ldots, x_m)$ be a polynomial in m variables. The evaluation map of f on A is defined as

$$ev_A : \mathbb{F}_q[x_1, x_2, \ldots, x_m] \to \mathbb{F}_q^n$$

where

$$ev_A(f) = (f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n)).$$

We remark that the vanishing ideal of A, namely

$$I_A = \{f \in \mathbb{F}_q[x_1, x_2, \ldots, x_m] \mid f(\alpha) = 0 \forall \alpha \in A\},$$

is the kernel of the evaluation map ev_A.

Let $A = \{\alpha_1, \alpha_2, \ldots, \alpha_n\} \subseteq \mathbb{F}_q^m$. Let L be a subspace of $\mathbb{F}_q[x_1, x_2, \ldots, x_m]$. The set

$$C(A, L) = \{ev_A(f) \mid f \in L\}$$

is known as an affine variety code. The definition of an affine variety code simply states that a linear code may be constructed by evaluating functions on a set of points. In most cases, the structure of L or A will imply certain properties of the code hold, such as dimension, minimum distance or locality.

Lemma 1. *Let $V_1 \subseteq \mathbb{F}_q^{m_1}$. Let L_1 be a subspace of $\mathbb{F}_q[x_1, x_2, \ldots, x_{m_1}]$. Similarly, take $V_2 \subseteq \mathbb{F}_q^{m_2}$ and L_2 be a subspace of $\mathbb{F}_q[y_1, y_2, \ldots, y_{m_2}]$. Consider the evaluation codes: $C_1 = C(V_1, L_1)$ and $C_2 = C(V_2, L_2)$. The product code $C_1 \times C_2$ is the evaluation code $C_3 = C(V_3, L_3)$, where $V_3 = V_1 \times V_2 \subseteq \mathbb{F}_q^{m_1+m_2}$ and the set of evaluated functions is $L_3 = \{f(X)g(Y), f \in L_1, g \in L_2\}$.*

Proof. It is clear that taking $f \in L_1$ and $g \in L_2$ and evaluating the product $f(X)g(Y)$ on the array $\{(\alpha, \beta) \mid \alpha \in V_1, \beta \in V_2\}$ will give a codeword of the form $(f(\alpha)g(\beta))$. This codeword is also a codeword of $C_1 \times C_2$.

In order to prove equality, we use a dimensional analysis. As C_1 is a code of dimension k_1, there exist $f_1, f_2, \ldots, f_{k_1}$ functions of L_1 and $\alpha_1, \alpha_2, \ldots, \alpha_{k_1} \in V_1$ such that $f_i(\alpha_j) = \delta_{i,j}$. Likewise, there exist $g_1, g_2, \ldots, g_{k_2}$ functions of L_2 and $\beta_1, \beta_2, \ldots, \beta_{k_2} \in V_2$ such that $g_{i'}(\beta_{j'}) = \delta_{i',j'}$. The evaluation of the functions $f_i g_{i'}$ on the points $\alpha_j \beta_{j'}$ will also imply the image has dimension $k_1 k_2$.

We will construct LRC codes based on the product code of the Tamo–Barg construction and Lemma 1. In particular, we shall take $V_1 \times V_2, V_1 \times V_2 \times V_3$, for $V_i \subseteq \mathbb{F}_q$ as our evaluation sets and the evaluation functions to be

$$\{f_1(X)f_2(Y)f_3(Z) \mid f_i \in L_i\}$$

where $L_i = \{T^a g_i(T)^j, 0 \leq a \leq r_i, a \neq s_i, a + (r_i + 1)j < k'\}$.

Note that classical Hermitian codes are obtained by evaluating monomials of the form $\mathcal{M}(s) := \{X^i Y^j \mid iq + j(q+1) \leq s\}$ on the q^3 points of the form $A = \{(\alpha, \beta) \in \mathbb{F}_{q^2}^2 \mid \alpha^{q+1} = \beta^q + \beta, \alpha \neq 0\}$. However, as the vanishing ideal of A is the ideal spanned by $X^{q+1} - Y^q - Y$ and $X^{q^2-1} - 1$, we may consider the Hermitian code obtained by evaluating the functions

$$\mathcal{M}(s) = \{X^i Y^j \mid iq + j(q+1) \leq s, 0 \leq i \leq q^2 - 2, 0 \leq j \leq q - 1\}.$$

In order to find a subcode of the Hermitian code with a given locality, proceed as follows: Let $g_1(x)$ be a polynomial of degree $r_1 + 1$. Let $A_1, A_2, \ldots, A_{\frac{q^2-1}{r_1+1}}$ be a partition of $\mathbb{F}_{q^2}$ into multiplicative cosets of $\mathbb{F}_{q^2}^*$ where $g_1(X)$ is constant on each A_i. Likewise let $g_2(Y)$ be a polynomial of degree $r_2 + 1$. Let $B_1, B_2, \ldots, B_{\frac{q}{r_2+1}}$ be a partitiion of $\{\gamma | \gamma^q + \gamma = 0\}$ where $g_2(Y)$ is constant on each B_j. For fixed s_1, s_2, the code obtained by evaluating

$$L_{s1,s2}(s) = \left\{ X^{i_1} g_1(X)^{i_2} Y^{j_1} g_2(Y)^{j_2} \mid \begin{array}{l} 0 \leq i_1 \leq r_1, i_1 \neq s_1, 0 \leq j_1 \leq r_2, \\ 0 \leq i_1 + (r_1 + 1)i_2 \leq q^2 - 2, \\ 0 \leq j_1 + (r_2 + 1)j_2 \leq q - 1 \end{array} \right\}$$

is a subcode of the Hermitian code of degree s which also has locality r_1 and locality r_2 with availability 2. In this case we obtain the codes over $\mathbb{F}_{16}$ with locality

3 and availability 2 and the following parameters: $[64, 1, 64]$, $[64, 2, 60]$, $[64, 3, 59]$, $[64, 4, 56]$, $[64, 5, 55]$, $[64, 6, 54]$, $[64, 7, 51]$, $[64, 8, 50]$, $[64, 9, 48]$, $[64, 10, 46]$, $[64, 11, 44]$, $[64, 12, 43]$, $[64, 13, 40]$, $[64, 14, 39]$, $[64, 15, 38]$, $[64, 16, 35]$, $[64, 17, 34]$, $[64, 18, 32]$, $[64, 19, 30]$, $[64, 20, 28]$, $[64, 21, 27]$, $[64, 22, 24]$, $[64, 23, 23]$, $[64, 24, 22]$, $[64, 25, 19]$, $[64, 26, 18]$, $[64, 27, 16]$, $[64, 28, 14]$, $[64, 29, 12]$, $[64, 30, 12]$, $[64, 31, 8]$, $[64, 32, 8]$, $[64, 33, 8]$, $[64, 34, 6]$, $[64, 35, 6]$, $[64, 36, 4]$. Note these codes handily outperform the product code construction from two Reed–Solomon code over $\mathbb{F}_{16}$, which have parameters: $[64, 3, 56]$, $[64, 6, 42]$, $[64, 9, 28]$, $[64, 12, 30]$, $[64, 18, 20]$, $[64, 27, 12]$.

For Suzuki curves, we use two different constructions of LRCs. As the full affine plane $\mathbb{F}_q^2$ is the set of $\mathbb{F}_q$–rational points, we evaluate the intersection of a product code of two LRC codes with the Suzuki code of length q^2. The vanishing ideal of the full affine plane is the ideal spanned by $X^q - X, Y^q - Y$. In this case, the Suzuki code is obtained by taking the polynomials of low order at infinity and evaluating at the q^2 rational points. One can also take the remainders modulo $X^q + X, Y^q + Y$ to determine the dimension of the code instead. Hence the Suzuki code is obtained by evaluating $L(s) =$

$$\{X^a Y^b U^c V^d \mod X^q + X, Y^q + Y \mid aq + b(q+q_0) + c(q+2q_0) + d(q+2q_0+1) \le s\}.$$

In this case, the optimal LRC codes of locality 3 and length 8 have parameters: $[8, 1, 8]$, $[8, 2, 7]$, $[8, 3, 6]$, $[8, 4, 4]$, $[8, 5, 3]$, $[8, 6, 2]$. In order to get a product code of locality 3 and availability 2 from these codes, we get a $[64, 10, 21]$ code. From the Suzuki code construction, after imposing additional LRC conditions, we get a $[64, 10, 36]$ code with the same locality and availability parameters.

In the following table, we compare some Suzuki LRC codes with some RS product LRC codes. Both have the same length, symbols, locality and availability. Note that we were able to improve on most of the Product code constructions, except for $[64, 25, 9]$. We expect to improve our codes by improving the minimum distance bounds of the Suzuki codes.

To get LRCs from the Ree curve we shall make a similar construction to the codes from the Suzuki curve. Due to the abundance of possible codes and availabilities, we shall restrict ourselves to the case where $q = 27$, availability is 3 and $r_1 = r_2 = r_3 = 8$. Please recall that the Ree curve R_q may be described by the equation

$$R_q : \begin{cases} y^q - y = x^{q_0}\,(x^q - x) \\ z^q - z = x^{2q_0}\,(x^q - x) \end{cases}$$

where $q_0 = 3^s$, $q = 3q_0^2$, and $s \in \mathbb{N}$. The valuation of x at infinity is q, the valuation of y at infinity is $q + q_0$ and the valuation of z at infinity is $q + 2q_0$. If G represents the pole at infinity of the Ree curve, and D is the divisor corresponding to the $\mathbf{F}_{27}$–affine points of the Ree curve, then the code $C(sG, D)$ is the algebraic geometry code obtained by evaluating all functions having poles only at infinity of order $\le s$. We shall compare LRC subcodes of $C(sG, D)$ with product codes of Reed–Solomon codes. We shall use a particular Tamo–Barg construction [21] for $\mathbf{F}_{27}$. In this case, our sets will be places where the trace is

$[s_1, s_2]$	Suzuki code	Suzuki code with locality and availability
$[1, 0]$	$[64, 1, 64]$	$[64, 1, 64]$
$[1, 0]$	$[64, 2, 56]$	$[64, 2, 56]$
$[2, 0]$	$[64, 3, 54]$	$[64, 3, 54]$
$[3, 0]$	$[64, 5, 51]$	$[64, 4, 51]$
$[3, 0]$	$[64, 6, 48]$	$[64, 5, 48]$
$[3, 0]$	$[64, 7, 46]$	$[64, 6, 46]$
$[3, 0]$	$[64, 8, 44]$	$[64, 7, 44]$
$[3, 0]$	$[64, 12, 40]$	$[64, 8, 40]$
$[3, 0]$	$[64, 14, 38]$	$[64, 9, 38]$
$[3, 0]$	$[64, 15, 36]$	$[64, 10, 36]$
$[2, 0]$	$[64, 19, 32]$	$[64, 11, 32]$
$[3, 0]$	$[64, 20, 31]$	$[64, 12, 31]$
$[3, 0]$	$[64, 21, 30]$	$[64, 13, 30]$
$[3, 0]$	$[64, 23, 28]$	$[64, 14, 28]$
$[3, 0]$	$[64, 24, 27]$	$[64, 15, 27]$
$[3, 0]$	$[64, 25, 26]$	$[64, 16, 26]$
$[3, 0]$	$[64, 27, 24]$	$[64, 17, 24]$
$[3, 0]$	$[64, 29, 22]$	$[64, 18, 22]$
$[3, 0]$	$[64, 31, 20]$	$[64, 19, 20]$
$[3, 0]$	$[64, 32, 19]$	$[64, 20, 19]$
$[3, 0]$	$[64, 35, 16]$	$[64, 21, 16]$
$[3, 0]$	$[64, 37, 14]$	$[64, 22, 14]$
$[3, 0]$	$[64, 39, 12]$	$[64, 23, 12]$
$[3, 0]$	$[64, 40, 11]$	$[64, 24, 11]$
$[3, 0]$	$[64, 43, 8]$	$[64, 25, 8]$
$[3, 0]$	$[64, 44, 7]$	$[64, 26, 7]$
$[3, 0]$	$[64, 45, 6]$	$[64, 27, 6]$
$[3, 0]$	$[64, 47, 4]$	$[64, 28, 4]$
$[3, 0]$	$[64, 49, 2]$	$[64, 29, 2]$

Table 1. Comparison of parameters of codes from the Suzuki curve using a standard AG code construction and those with locality and availability

Suzuki code with locality and availability	Comparable Product code
$[64, 1, 64]$	$[64, 1, 64]$
$[64, 2, 56]$	$[64, 2, 56]$
$[64, 3, 54]$	$[64, 3, 48]$
$[64, 4, 51]$	$[64, 4, 49]$
$[64, 5, 48]$	$[64, 5, 24]$
$[64, 6, 46]$	$[64, 6, 42]$
$[64, 7, 44]$	$[64, 6, 42]$
$[64, 8, 40]$	$[64, 8, 28]$
$[64, 9, 38]$	$[64, 9, 36]$
$[64, 10, 36]$	$[64, 10, 21]$
$[64, 11, 32]$	$[64, 10, 21]$
$[64, 12, 31]$	$[64, 12, 24]$
$[64, 13, 30]$	$[64, 12, 24]$
$[64, 14, 28]$	$[64, 12, 24]$
$[64, 15, 27]$	$[64, 15, 18]$
$[64, 16, 26]$	$[64, 16, 16]$
$[64, 17, 24]$	$[64, 16, 16]$
$[64, 18, 22]$	$[64, 18, 12]$
$[64, 19, 20]$	$[64, 18, 12]$
$[64, 20, 19]$	$[64, 20, 12]$
$[64, 21, 16]$	$[64, 20, 12]$
$[64, 22, 14]$	$[64, 20, 12]$
$[64, 23, 12]$	$[64, 20, 12]$
$[64, 24, 11]$	$[64, 24, 8]$
$[64, 25, 8]$	$[64, 25, 9]$
$[64, 26, 7]$	$[64, 25, 9]$
$[64, 27, 6]$	$[64, 25, 9]$
$[64, 28, 4]$	$[64, 25, 9]$
$[64, 29, 2]$	$[64, 25, 9]$

Table 2. Comparison of parameters of codes from the Suzuki curve with locality and availability and product codes

constant $A_0 = \{a \in \mathbf{F}_{27} \mid a + a^3 + a^9 = 0\}$, $A_1 = \{a \in \mathbf{F}_{27} \mid a + a^3 + a^9 = 1\}$ and $A_2 = \{a \in \mathbf{F}_{27} \mid a + a^3 + a^9 = 2\}$. The polynomial $L(T) = T + T^3 + T^9$ is constant on the recovery sets A_0, A_1, A_2 and the evaluation of the polynomials in $\{L(T)^i T^j \mid 0 \le i \le 2, 0 \le j \le 7, 2i + j \le k\}$ gives a subcode of the Reed–Solomon code $RS_{27}(\mathbf{F}_{27}, k)$ which is an LRC with locality 8.

The possible Reed–Solomon codes with locality 8 and length 27 of this form are: $[27, 1, 27]$, $[27, 2, 26]$, $[27, 3, 25]$, $[27, 4, 24]$, $[27, 5, 23]$, $[27, 6, 22]$, $[27, 7, 21]$, $[27, 8, 20]$, $[27, 9, 18]$, $[27, 10, 17]$, $[27, 11, 16]$, $[27, 12, 15]$, $[27, 13, 14]$, $[27, 14, 13]$, $[27, 15, 12]$, $[27, 16, 11]$, $[27, 17, 9]$, $[27, 18, 8]$, $[27, 19, 7]$, $[27, 20, 6]$, $[27, 21, 5]$, $[27, 22, 4]$, $[27, 23, 3]$, $[27, 24, 2]$.

The key idea of this proof is that both the product code of Reed–Solomon codes and the subcodes of the Ree AG code may be considered as evaluation codes of combinations of monomials in $\mathcal{L} = \{X^i Y^j Z^l \mid 0 \le i, j, l \le 26\}$. In the $\mathbf{F}_{27}^3$.

The subcode of $C(sG, D)$ is obtained by evaluating the monomials in

$$\mathcal{L}(s) = \{X^a Y^b Z^c \in \mathcal{L} \mid aq + b(q + q_0) + c(q + 2q_0) \le s, 0 \le a, b, c \le q - 1\}.$$

The subcode of $C(sG, D)$ with locality 8 and availability 3 is given by evaluating polynomials of the form $L(X)^{a1} X^{a_2} L(Y)^{b1} Y^{b2} L(Z)^{c1} Z^{c2}$ where $0 \le a_1, b_1, c_1 \le 2, 0 \le a_2, b_2, c_2 \le 7$ and subject to the degree constrain that the polynomials should also be in $\mathcal{L}(s)$. Note that depending on the parameters of the codes we might find better Reed–Solomon product codes as LRCs or better LRC subcodes from the Ree curve.

For example, comparing codes with minimum distance 600 we get an LRC with parameters $[19683, 4536, 600]$, locality 8 and availability 3 from the product code construction of the Reed–Solomon code and a $[19683, 2937, 600]$ LRC with locality 8 and availability 3 from $C(sG, D)$. However, comparing codes with dimension 200 we get a $[19683, 200, 10580]$ LRC with locality 8 and availability 3 from the product code construction of the Reed–Solomon code and a $[19683, 201, 13086]$ LRC with locality 8 and availability 3 from the AG code.

There is also an LRC construction using the codes $C(sG, D)$. In this case note that for the same replication sets A_0, A_1 and A_2, the dual code of an LRC with locality 8 is generated by evaluating $\{L(T)^i \mid 0 \le i \le 2\}$. If we extend this to $\mathbf{F}_{27}^3$ we can get a code with locality 8 and availability 3 as the dual code of the evaluation of $\{L(X)^i L(Y)^j L(Z)^k \mid 0 \le i \le 2\}$. In order to find subcodes of $C(sG, D)$ with locality 8 and availability 3 we consider how many of the functions $\{L(X)^i L(Y)^j L(Z)^k \mid 0 \le i \le 2\}$ also have weight s. The dimension of the LRC is found by computing the dimension of $\mathcal{L}(s) + \{L(X)^i L(Y)^j L(Z)^k \mid 0 \le i \le 2\}$.

In this case we have found a $[19683, 4536, 600]$ LRC with locality 8 and availability 3 from the product code construction of the Reed–Solomon code and a $[19683, 15434, 600]$ LRC with locality 8 and availability 3 from $C(sG, D)^{\perp}$.

We have found instances in which the Reed–Solomon product codes are better than the LRC from the AG codes. Likewise, we have found cases in which the AG LRCs outperform the Reed–Solomon codes. Further improvements could be possible as knowledge of the Riemann-Roch spaces of the Ree curve improves.

References

1. Barg, A., Haymaker, K., Howe, E., Matthews, G. L., Varilly-Alvarado A.: Locally recoverable codes from algebraic curves and surfaces, in Algebraic Geometry for Coding Theory and Cryptography, E.W. Howe, K.E. Lauter, and J.L. Walker, Editors, Springer, 2017, pp. 95–126. doi: 10.1007/978-3-319-63931-4_4
2. Ballentine, S., Barg, A., Vlăduţ, S.: Codes with hierarchical locality from covering maps of curves, IEEE Transactions on Information Theory, vol. 65, no. 10, pp. 6056–6071, Oct. 2019. doi: 10.1109/TIT.2019.2919830
3. Eid, A., Duursma, I.: Smooth embeddings for the Suzuki and Ree curves. Algorithmic arithmetic, geometry, and coding theory, vol. 637, 251-291, 2015. doi: 10.1090/conm/637/12763
4. Eid, A., Hasson, H., Ksir, A. , Peachey, J.: Suzuki-invariant codes from the Suzuki curve. Designs, Codes and Cryptography, vol. 81, pp. 413– 425, 2016. doi: 10.1007/s10623-015-0164-5
5. Giulietti, M., Korchmros, G.: A new family of maximal curves over a finite field, Mathematische Annalen, vol. 343, article 229, 2009. doi: 10.1007/s00208-008-0270-z
6. Giulietti, M., Montanucci, M., Quoos, L., Zini, G.: On some Galois covers of the Suzuki and Ree curves, Journal of Number Theory, vol. 189, pp. 220–254. doi: 10.1016/j.jnt.2017.12.005.
7. Guruswami, V., Jin, L., Xing, C.: Constructions of maximally recoverable local reconstruction codes via function fields, International Colloquium on Automata, Languages, and Programming, 2019. doi: 10.4230/LIPIcs.ICALP.2019.68
8. Hansen, J.P., Stichtenoth, H.: Group codes on certain algebraic curves with many rational points, Applicable Algebra in Engineering, Communication and Computing, vol. 1, pp. 67–77, 1990. doi: 10.1007/BF01810849
9. Haymaker, K., Malmskog, B., Matthews, G. L.: Locally recoverable codes with availability $t \geq 2$ from fiber products of curves, Advances in Mathematics of Communications, vol. 12 (2), pp. 317–336, 2018. doi: 10.3934/amc.2018020
10. Hirschfeld, J., Korchmáros, G., Torres, F, Algebraic Curves over a Finite Field, PRINCETON; OXFORD: Princeton University Press, 2008. doi:10.2307/j.ctt1287kdw
11. Jin, L., Ma, L., Xing, C.: Construction of optimal locally repairable codes via automorphism groups of rational function fields, IEEE Transactions on Information Theory, vol. 66, no. 1, pp. 210–221, Jan. 2020. doi: 10.1109/TIT.2019.2946637
12. Kirfel, C., Pellikaan, R.: The minimum distance of codes in an array coming from telescopic semigroups, IEEE Transactions on Information Theory, vol. 41, no. 6, pp. 1720–1732, Nov. 1995. doi: 10.1109/18.476245
13. Li, X., Ma, L., and Xing, C.: Optimal locally repairable codes via elliptic curves, IEEE Transactions on Information Theory, vol. 65, no. 1, pp. 108–117, Jan. 2019. doi: 10.1109/TIT.2018.2844216
14. López, H., Matthews, G. L., Soprunov, I.: Monomial-Cartesian codes and their duals, with applications to LCD codes, quantum codes, and locally recoverable codes, Designs, Codes and Cryptography, 2020. doi:10.1007/s10623-020-00726-x
15. Matthews, G. L.: Codes from the Suzuki function field. IEEE Transactions on Information Theory, vol. 50, no. 12, pp. 3298–3302, Dec. 2004. doi: 10.1109/TIT.2004.838102.
16. Montanucci, M., Timpanella, M., Zini, G.: AG codes and AG quantum codes from cyclic extensions of the Suzuki and Ree curves, Journal of Geometry, vol. 109, article 23, 2018. doi: 10.1007/s00022-018-0428-0.

17. Pedersen, J. P.: A function field related to the Ree group, Coding theory and algebraic geometry (Luminy, 1991), Lecture Notes in Math., vol. 1518, Springer, Berlin, 1992, pp. 122–31. doi: 10.1007/BFb0087997
18. Skabelund, D. C.: New maximal curves as ray class fields over Deligne-Lusztig curves. Proceedings of the American Mathematical Society, vol. 146, no. 2, pp. 525–540. doi: 10.1090/proc/13753
19. Tafazolian, S., Torres, F.: On the Ree curve, Journal of Pure and Applied Algebra, vol. 223, no. 9, pp. 3831–3842, 2019. doi: 10.1016/j.jpaa.2018.12.006
20. Tamo, I., Barg, A.: Bounds on locally recoverable codes with multiple recovering sets, 2014 IEEE International Symposium on Information Theory, Honolulu, HI, 2014, pp. 691-695. doi: 10.1109/ISIT.2014.6874921
21. Tamo, I., Barg, A.: A Family of Optimal Locally Recoverable Codes, IEEE Transactions on Information Theory, vol. 60, no. 8, pp. 4661–4676, Aug. 2014. doi: 10.1109/TIT.2014.2321280
22. Barg, A., Tamo, I., Vlăduţ: Locally Recoverable Codes on Algebraic Curves, IEEE Transactions on Information Theory, vol. 63, no. 8, pp. 4928-4939, Aug. 2017. doi: 10.1109/TIT.2017.2700859
23. Tsfasman, M., Vlăduţ, S., Zink, T.: Modular curves, Shimura curves and Goppa codes better than Varshamov-Gilbert bound, Mathematische Nachrichten, vol. 109, pp. 21–28, 1982. doi: 10.1002/mana.19821090103